UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/800,202	03/12/2004	George Luis Wood	WELL0040	2368

22862 7590 11/19/2007

GLENN PATENT GROUP
3475 EDISON WAY, SUITE L
MENLO PARK, CA 94025

EXAMINER	
LIU, ALAN Y	

ART UNIT	PAPER NUMBER
4127	

MAIL DATE	DELIVERY MODE
11/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/800,202	WOOD ET AL.	
	Examiner	Art Unit	
	Alan Liu	4127	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/12/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This communication is a first Office Action Non-Final rejection on the merits. Claims 1-8, as originally filed, are currently pending and have been considered below.

Claim Objections

2. Claim 1 is objected to because of the following informalities: On line 15, "enters" should be changed to "enter".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. **Claims 4 and 8** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Terms used in claims 4 and 8 (Slot, DES, KD, MFK, KPE) need to be more clearly defined to make the encryption method disclosed comprehensible.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. **Claims 1-8** are rejected under 35 U.S.C. 102(b) as being anticipated by Hodgson et al. (2002/0123972).

As per claim 1, Hodgson et al. teaches a system for making a purchase transaction by PIN purchasing over the Internet comprising (see Abstract):

a merchant's check out web page on a merchant server for a buyer to make a purchase from the buyer's browser (page 3, paragraph 0035; via Internet merchant server 20 and a merchant web site is browsed by a user who initiates a secure payment transaction);

means for the buyer selecting PIN purchase as a payment method and for entering a debit card number (Figure 6; page 7, paragraph 0092; via choosing credit or debit and manual entry of a credit card number);

an Internet authorization server to which the merchant system re-directs said buyer's browser and to which the merchant system passes along a unique transaction id coupled to said transaction (page 3, paragraphs 0028-0029, via transmitting FP block to Secure Transaction Management Server, STMS; page 8, paragraph 0108, via merchant/consumer tracking number assigned to track consumer's order) ;

means for said Internet authorization server displaying a secure PIN pad screen and using a unique session key (page 3, paragraph 0026, via PIN/PAD incorporated into the consumer's Internet access device; page 7, paragraph 0100, via Data Encryption session key);

an input device for the buyer to enters a PIN (input device 1114);

means for encrypting said using said unique session key (page 7, paragraph 0100, via RSA public key encryption with DES session key);

a host security module to which said Internet authorization server passes said encrypted PIN, said host security module generating an encrypted ANSI PIN block (Figure 1; page 3, paragraphs 0026-0030; via Hardware Security Module deencrypts and reencrypts the PIN block);

means for said ANSI PIN block passing back to said Internet authorization server (Figure 1, via connection between HSM and STMS);

means for said Internet authorization server returning control of said buyer's browser to said merchant server and passing along said unique transaction id (page 6, paragraphs 0084-0085, via "AUTH" response sent to consumer's PC; page 8, paragraph 0108, via merchant/consumer tracking number);

a payment request based on contents of a shopping cart and said payment method, wherein said payment request is created by said merchant server (page 3, paragraph 0033, via after the consumer has filled their shopping cart, a secure payment is initiated and a script is sent from the merchant web site to the consumer's browser);

an Internet payments server to which said merchant server sends said payment request, wherein said Internet payments server determines said payment type and formats a payment authorization request (page 3, paragraphs 0028-0029, via FP block containing transaction information is sent to STMS, where a transaction request is sent to the payment processor);

an ATM/POS system to which said payment authorization request is routed, wherein said ATM/POS system takes said encrypted ANSI PIN block passed along with said payment request and routes said ANSI PIN block through a second host secure module to be decrypted and translated (page 5, paragraph 0061, via STMS forwards payment transaction to a POS transaction processor that has an HSM which can decrypt data sent by the HSM attached to the STMS);

a data deposit account system wherein if said transaction is an on-us transaction, then said ATM/POS system validates said PIN and passes a transaction amount coupled to said transaction to said associated data deposit account system for authorization (Figure 12; via connections to STAR 1240 and NYCE 1250, which are ATM groups);

a network coupled to the buyer's issuing financial institution, wherein if said transaction is an off-us transaction, then said authorization request is routed to said network to be further routed to said buyer's issuing financial institution (Figure 12; via connections to VISA 1220 and Mastercard 1230, which connects to issuing bank);

means for passing back to said ATM/POS system and finally back to said merchant server an authorization approval or denial (page 6, paragraph 0081, via POS processor obtains "AUTH" response from issuing bank and passes it to the STMS).

As per claim 2, Hodgson et al. teaches that the unique session is under Secure Sockets Layer (SSL) technology (page 6, paragraph 0076, via message encrypted with 128bit SSL).

As per claim 3, Hodgson et al. teaches that a link between said Internet authorization server and said Internet payments server is a secure link (page 10, paragraph 152, via secure connections).

As per claim 4, Hodgson et al. teaches that the means for encrypting a user's PIN further comprises:

means for an Internet authorization server receiving control of a browser of said user from a merchant server, and receiving data comprising: merchant id, transaction id, return URL, and a merchant defined as its own entity and which does not contain the user's PIN (page 8, paragraph 0108, via transaction request with parameters including merchant number, merchant/consumer tracking number, and follow-up URL);

means for said Internet authorization server initiating a call to a host secure module to request a public key (page 8, paragraph 0101, via public key encryption);

means for said host secure module returning public key plus additional data (page 3, paragraph 0030, via HSM deencrypting and reencrypting PIN block);

means for said Internet authorization server passing JavaScript and the public key back to said browser (page 3, paragraph 0033, via script sent to consumer's browser; page 6, paragraph 0074, via using public key encryption);

means for said user entering and submitting a PIN, wherein digits are hidden; (pages 5-6, paragraphs 0072-0073, via entering PIN using DES network standards where PIN is never "in the clear");

means for generating a DES key at said browser, encrypting said entered PIN digits, encrypting the DES key using the public key, and posting to said IAS (page 6,

paragraphs 0073-0076; page 7, paragraph 0100; via loading a DES session key and using RSA public key encryption to encrypt PIN along with other data into a data block that is transmitted to the STMS);

means for said Internet authorization server passing encrypted data to said host secure module (Figure 1; page 3, paragraph 0030, via encrypted PIN block to be translated by HSM);

means for said host secure module converting to create a standard ANSI PIN block (page 3, paragraphs 0026-0030, via encrypting into a block meeting ANSI network requirements);

means for said host secure module passing back to said IAS (page 3, paragraph 0030, via HSM connected to STMS translates the PIN block);

and means for said Internet authorization server storing in a database (transaction database 0110; pages 8-9, paragraph 0110-0135, via information including transaction number, time of initial entry, and PIN/PAD serial number).

As per claim 5, Hodgson et al. teaches a method for making a purchase transaction by PIN purchasing over the Internet, said method comprising the steps of (see Abstract):

a buyer proceeding to a merchant's checkout page on a merchant server from a buyer's browser to make a purchase (page 3, paragraph 0035; via Internet merchant server 20 and a merchant web site is browsed by a user who initiates a secure payment transaction);

said buyer selecting PIN Purchase as a payment method and entering an associated debit card number (Figure 6; page 7, paragraph 0092; via choosing credit or debit and manual entry of a credit card number);

said merchant server re-directing said buyer's browser to an Internet authorization server and passing a unique transaction id coupled to said transaction (page 3, paragraphs 0028-0029, via transmitting FP block to Secure Transaction Management Server, STMS; page 8, paragraph 0108, via merchant/consumer tracking number assigned to track consumer's order);

said Internet authorization server displaying a secure PIN pad screen and using a unique session key (page 3, paragraph 0026, via PIN/PAD incorporated into the consumer's Internet access device; page 7, paragraph 0100, via Data Encryption session key);

said buyer entering said PIN using an input device (input device 1114);

encrypting said PIN using said unique session key (page 7, paragraph 0100, via RSA public key encryption with DES session key);

said Internet authorization server passing said encrypted PIN to a host secure module, wherein said host secure module generates an associated encrypted ANSI PIN block (Figure 1; page 3, paragraphs 0026-0030; via Hardware Security Module deencrypts and reencrypts the PIN block);

said Internet authorization server returning control of said buyer's browser to said merchant server along with said unique transaction id (page 6, paragraphs 0084-0085,

via "AUTH" response sent to consumer's PC; page 8, paragraph 0108, via merchant/consumer tracking number);

said merchant server creating a payment request based on contents of said shopping cart and said payment method, wherein said merchant server sends said payment request to an Internet payments server (page 3, paragraph 0033, via after the consumer has filled their shopping cart, a secure payment is initiated and a script is sent from the merchant web site to the consumer's browser; page 6, paragraph 0076, via message is transmitted to STMS);

said Internet payments server determining a payment type and formatting a payment authorization request (page 3, paragraphs 0028-0029, via FP block containing transaction information is sent to STMS, where a transaction request is sent to the payment processor);

said payment authorization request routing to an ATM/POS system, wherein said ATM/POS system takes said encrypted ANSI PIN block and routes it through a second host secure module to be decrypted and translated to an acquiring financial institution's encrypted PIN data (page 5, paragraph 0061, via STMS forwards payment transaction to a POS transaction processor that has an HSM which can decrypt data sent by the HSM attached to the STMS);

if said transaction is on-us, then said ATM/POS system validating said PIN and passing an associated transaction amount to a data deposit account system for authorization (Figure 12; via connections to STAR 1240 and NYCE 1250, which are ATM groups);

if said transaction is off-us, then said authorization request routing to a network for routing to an issuing financial institution of said buyer (Figure 12; via connections to VISA 1220 and Mastercard 1230, which connects to issuing bank);

passing back to said ATM/POS system an authorization approval or denial, wherein said authorization approval or denial is routed to said Internet payments server and finally back to said merchant server (page 6, paragraph 0081, via POS processor obtains "AUTH" response from issuing bank and passes it to the STMS).

As per claim 6, Hodgson et al. teaches that the unique session is under Secure Sockets Layer (SSL) technology (page 6, paragraph 0076, via message encrypted with 128bit SSL).

As per claim 7, Hodgson et al. teaches that a link between said Internet authorization server and said Internet payments server is a secure link (page 10, paragraph 152, via secure connections).

As per claim 8, Hodgson et al. teaches encrypting a user's PIN further comprises the steps of:

an Internet authorization server receiving control of a browser of said user from a merchant server, and receiving data comprising: merchant id, transaction id, return URL, and a merchant defined as its own entity and which does not contain the user's PIN (page 8, paragraph 0108, via transaction request with parameters including merchant number, merchant/consumer tracking number, and follow-up URL);

said Internet authorization server initiating a call to a host secure module to request a public key (page 8, paragraph 0101, via public key encryption);

said host secure module returning public key plus additional data (page 3, paragraph 0030, via HSM deencrypting and reencrypting PIN block);

said Internet authorization server passing JavaScript and the public key back to said browser (page 3, paragraph 0033, via script sent to consumer's browser; page 6, paragraph 0074, via using public key encryption);

said user entering and submitting a PIN, wherein digits are hidden (pages 5-6, paragraphs 0072-0073, via entering PIN using DES network standards where PIN is never "in the clear");

generating a DES key at said browser, encrypting said entered PIN digits, encrypting the DES key using the public key, and posting to said IAS (page 6, paragraphs 0073-0076; page 7, paragraph 0100; via loading a DES session key and using RSA public key encryption to encrypt PIN along with other data into a data block that is transmitted to the STMS);

said Internet authorization server passing encrypted data to said host secure module (Figure 1; page 3, paragraph 0030, via encrypted PIN block to be translated by HSM);

said host secure module converting to create a standard ANSI PIN block (page 3, paragraphs 0026-0030, via encrypting into a block meeting ANSI network requirements);

said host secure module passing said MFK(KPE) + KPE(PIN) back to said IAS (page 3, paragraph 0030, via HSM connected to STMS translates the PIN block);

and said Internet authorization server storing in a database (transaction database 0110; pages 8-9, paragraph 0110-0135, via information including transaction number, time of initial entry, and PIN/PAD serial number).

37 CFR § 1.105 Requirement for Information

Applicants and the assignee of this application are required under 37 CFR 1.105 to provide the following information that the examiner has determined is reasonably necessary to the examination of this application.

This information is required to complete the record so that an analysis can be made under 35 U.S.C. 102 and 103 may be ascertained. Thus, the following information is requested:

- Information regarding the encryption algorithm disclosed in Claims 4 and 8. Some of the acronyms terms are unclear and should be more explicitly defined.

The fee and certification requirements of 37 C.F.R. § 1.97 are waived for those documents submitted in reply to this requirement. This waiver extends only to those documents within the scope of this requirement under 37 C.F.R. § 1.105 that are included in the applicant's first complete communication responding to this requirement. Any supplemental replies subsequent to the first communication responding to this requirement and any information disclosures beyond the scope of this requirement under 37 C.F.R. § 1.105 are subject to the fee and certification requirements of 37 C.F.R. § 1.97.

The applicant is reminded that the reply to this requirement must be made with candor and good faith under 37 CFR 1.56. Where the applicant does not have or cannot readily obtain an item of required information, a statement that the item is unknown or cannot be readily obtained will be accepted as a complete response to the requirement for that item.

This requirement is an attachment of the enclosed Office action. A complete reply to the enclosed Office action must include a complete reply to this requirement. The time period for reply to this requirement coincides with the time period for reply to the enclosed Office action.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Lazzaro et al. (2003/0182558) discloses a dynamic pin pad for debit electronic transactions.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Alan Liu whose telephone number is 571-270-5113. The examiner can normally be reached on Monday through Thursday, 8:30AM-6:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lynda Jasmin can be reached on 571-270-3033. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AL

/Lynda Jasmin/
Supervisory Patent Examiner, Art Unit 4127